What is claimed is:

1. A method of detecting polymorphic viral code in a computer program, comprising the steps of:

(a) emulating a first predetermined number of instructions of the computer program;

(b) collecting information corresponding to a state of a plurality of registers and/or flags after each emulated instruction execution; and

(c) determining a probability that the computer program contains polymorphic viral code based on an heuristic analysis of the collected register/flag state information.

2. The method of claim 1, further comprising emulating a second predetermined number of instructions if the probability determined in step (c) is above a predetermined threshold, wherein the second predetermined number of instructions is greater than the first predetermined number of instructions.

3. The method of claim 2, wherein the second predetermined number of instructions corresponds to execution of a polymorphic decryptor.

4. The method of claim 1, further comprising monitoring the plurality of registers and/or flags for improper register/flag usage.

5. The method of claim 4, further comprising maintaining, for each of the plurality of registers and/or flags, a corresponding count of a number of times that the register/flag was improperly used during the emulation of instructions in step (a).

6. The method of claim 1, further comprising monitoring operand values of the instructions emulated in step (a).

7. The method of claim 6, further comprising detecting when an operand value of an instruction which is set is not used by the instruction.

8. The method of claim 6, further comprising detecting when an undefined operand of an instruction is used by the instruction.

9. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting polymorphic viral code in a subject computer program, the method steps comprising:

emulating a selected number of instructions of the computer program;

collecting information corresponding to a state of a plurality of registers/flags after each emulated instruction execution; and

determining a probability that the computer program contains polymorphic viral code based on an heuristic analysis of the collected register/flag state information.

10. A computer system, comprising:

a processor; and

a program storage device readable by the computer system, tangibly embodying a program of instructions executable by the processor to perform method steps for detecting polymorphic viral code in a subject computer program, the method steps comprising:

emulating a selected number of instructions of the computer program;

collecting and storing information corresponding to a state of a plurality of registers/flags after each emulated instruction execution; and

determining a probability that the computer program contains polymorphic viral code based on an heuristic analysis of the collected register/flag state information.

11. A computer data signal embodied in a transmission medium which embodies instructions executable by a computer to detect polymorphic viral code in a computer program comprising:

a first segment including emulator code to emulate a selected number of instructions of the computer program;

a second segment including analyzer code to analyze a plurality of registers/flags accessed during emulation of the instructions; and

a third segment including heuristic processor code to determine a probability that the computer program contains polymorphic viral code based on an heuristic analysis of register/flag state information supplied by the analyzer code.

12. An apparatus for detecting polymorphic viral code in a computer program, comprising:

an emulator, wherein the emulator emulates a first predetermined number of instructions of the computer program;

an operational code analyzer that analyzes a plurality of registers/flags accessed during emulation of the instructions; and

an heuristic analyzer, wherein the heuristic analyzer determines a probability that the computer program contains polymorphic viral code based on an heuristic analysis of register/flag state information supplied by the operational code analyzer.

13. The apparatus of claim 12, wherein the emulator emulates a second predetermined number of instructions if the probability determined by the heuristic analyzer is above a predetermined threshold, the second predetermined number of instructions being greater than the first predetermined number of instructions.

14. The apparatus of claim 13, wherein the second predetermined number of instructions corresponds to execution of a polymorphic decryptor.

15. The apparatus of claim 12, wherein the operational code analyzer monitors the plurality of registers and/or flags for improper register/flag usage.

16. The apparatus of claim 15, wherein the heuristic analyzer maintains, for each of the plurality of registers and/or flags, a corresponding count of a number of times that the register/flag was improperly used during the emulated instructions.

17. The apparatus of claim 12, wherein the operational code analyzer monitors operand values of the emulated instructions.

18. The apparatus of claim 17, wherein the operational code analyzer detects when an operand value of an instruction which is set is not used by the instruction.

19. The apparatus of claim 17, wherein the operational code analyzer detects when an undefined operand of an instruction is used by the instruction.